What is claimed is:

1. A system for implementing public key infrastructure (PKI) based encryption of content over an electronic network, comprising:

an encryption services component, the encryption services component generating key-pairs and providing certificate management services;

a PKI server, the PKI server being operable to function as at least one of a certificate authority and as a LDAP service provider;

a user information database;

a package database; and

a control server connected to the electronic network and operable to access the encryption services component, the PKI server, the user information database and the package database,

wherein the control server receives encrypted content in the form of a package,

wherein the package database stores the package,

wherein the package is sent back into the electronic network, and

wherein the package remains encrypted as it is passed through the control server and stored in the package database.

2. The system of claim 1, further comprising a notification server, wherein the notification server is operable to notify an intended recipient of the package that the package is awaiting pickup.

3. The system of claim 2, wherein the notification server is connected to at least one of an email server, a paging device, a netcall device, a facsimile machine and a voice line.

4. The system of claim 1, further comprising a transaction files database for tracking package traffic.

5. The system of claim 1, further comprising a roaming keys database.

6. The system of claim 1, further comprising an autoresponder, the autoresponder being operable to monitor a POP3 server and to notify the control server that an email sent in response to a notification server request was not successfully delivered.

7. The system of claim 1, further comprising an audit database.

8. The system of claim 1, wherein the control server is connected to the Internet.

9. The system of claim 8, wherein the control server is connected to the Internet via an SSL connection.

10. The system of claim 1, wherein the control server is operable to communicate with a local agent that is associated with an electronic device which itself is accessible via the electronic network.

11. The system of claim 1, wherein the content is at least one of an email message, an email attachment, a document, a business transaction, a graphic and streaming audio or video.

12. The system of claim 1, wherein the package comprises embedded dissemination rules that are not modifiable by a recipient of the package.

13. The system of claim 1, further comprising a certificate management component.

14. A secured content delivery system, comprising:

a control server, the control server being operable to receive encrypted content from an electronic network, the encrypted content having been encrypted using at least one public key and a private key, at least one public key and private key having previously been obtained via the control server;

a database server in communication with the control server, the database server being operable to store the encrypted content and store information indicative of a sender of the encrypted content and a recipient of the encrypted content; and

a notification server in communication with at least one of the control server and database server, the notification server being operable to notify the recipient of the encrypted content that the sender has sent encrypted content to the recipient,

wherein the public key is obtained without an express command from the sender.

15. The secured content delivery system of claim 14, further comprising a PKI server.

16. The secured content delivery system of claim 14, wherein the database server comprises at least one of a user information database, a transaction file database and an encrypted content database.

17. The secured content delivery system of claim 14, further comprising an encryption services module operable to generate key pairs and digital certificates that are compatible with a PKI.

18. The secured content delivery system of claim 14, wherein the control server receives the encrypted content from a local agent that is in communication with the electronic network.

19. The secured content delivery system of claim 14, wherein the control server communicates with a local agent to set up a communications link therebetween.

20. The secured content delivery system of claim 14, wherein the encrypted content is at least one of an email message, an email attachment, a document, a business transaction, a graphic and streaming audio or video.

21. The secured content delivery system of claim 14, wherein the electronic network is the Internet.

22. The secured content delivery system of claim 14, wherein the public key is obtained via an LDAP service.

23. In an electronic device having a messaging application capable of sending and receiving content over an electronic network, a system for sending and receiving encrypted content over the electronic network, comprising:

an application specific interface, the application specific interface being capable of interfacing with the messaging application to access and pass content and address information to and from the messaging application and update status information within the messaging application; and

a local agent in communication with the messaging application via the application specific interface, the local agent being operable to (i) receive unencrypted content from the messaging application, (ii) encrypt the content using a public/private key pair, and (iii) send encrypted content over the electronic network, the local agent further being operable to (iv) receive encrypted content from the electronic network, (v) launch a local agent-controlled window, (vi) decrypt the encrypted content using a private key, and (vii) display decrypted content in the local agent-controlled window.

24. The system of claim 23, wherein the application specific interface comprises software hooks providing access to the messaging application.

25. The system of claim 23, wherein the status information comprises entries in an inbox associated with the messaging application.

26. The system of claim 23, wherein the application specific interface is integrated with the local agent.

27. The system of claim 23, wherein the application specific interface is tailored to the messaging application.

28. The system of claim 23, wherein the local agent is operable to obtain the public key from a local register.

29. The system of claim 23, wherein the local agent is operable to automatically obtain the public key via a control server in communication with the electronic network.

30. The system of claim 23, wherein the local agent is operable to open the local agent-controlled window only after the local agent receives at least one of a passphrase and biometric authentication.

31. The system of claim 23, wherein at least one of the application specific interface and the local agent is operable to modify a graphical user interface of the messaging application.

32. The system of claim 23, wherein the local agent is operable to automatically preclude the viewing of the encrypted content in accordance with a dissemination rule wrapped with the encrypted content.

33. The system of claim 23, wherein the local agent is operable to wrap a dissemination rule with the encrypted content.

34. A system for implementing PKI-based encryption between a sender and a recipient, the system comprising:

a sender local agent associated with a sender electronic device, the sender electronic device being capable of connection to the Internet;

a recipient local agent associated with a recipient electronic device, the recipient electronic device being capable of connection to the Internet; and

a control server, the control server capable of being in communication with both the sender local agent and recipient local agent;

the sender local agent being operable to (i) receive content generated on the sender electronic device, (ii) generate a package of encrypted content using PKI-based encryption by obtaining at least one public key from one of the control server and a local registry, and (iii) send the package to the control server;

the control server being operable to receive the package from the sender local agent and transmit the package to the recipient local agent;

the recipient local agent being operable to (i) receive the package from the control server, (ii) launch a recipient local agent-controlled window, (iii) decrypt the encrypted content in the package, and (iv) display decrypted content within the recipient local agent-controlled window.

35. The system of claim 34, further comprising a package database for storing a plurality of packages.

36. The system of claim 34, further comprising a notification server component, the notification server component being operable to notify an intended recipient that a package is awaiting pickup.

37. The system of claim 34, wherein at least one of the sender local agent and the recipient local agent is an applet dynamically downloaded from the control server.

38. The system of claim 34, further comprising an application specific interface associated with at least one of the sender local agent and the recipient local agent.

39. The system of claim 34, further comprising a PKI server operable to at least one of generate public-private key-pairs and access keys via a LDAP service.

40. The system of claim 34, further comprising an audit database.

41. The system of claim 34, wherein the control server is operable to cause the package to be assigned a unique tracking number.

42. The system of claim 34, wherein the sender local agent is launched from within an email application.

43. The system of claim 34, wherein the sender local agent is operable to embed a content dissemination rule in the package.

44. The system of claim 43, wherein the dissemination rule comprises at least one of do not copy, do not print, do not forward and self-destruct.

45. The system of claim 34, wherein the content is at least one of an email, an email attachment, a data file, a music file, and an XML file.

46. The system of claim 34, wherein at least one of the sender local agent and recipient local agent is operating system independent.

47. The system of claim 34, wherein the control server controls at least one of security, authentication, tracking, confirmation and archiving.

48. The system of claim 36, wherein notification is provided by at least one of voice, fax pager and email.

49. The system of claim 34, wherein at least one of the sender local agent and recipient local agent is dynamically downloaded from the control server.

50. A system for presenting information, comprising:

a high volume package component operable to receive sequential data files and operable to associate the data files with a plurality of account and certificate data, respectively, to create a plurality of packages;

a high volume encryption component operable to implement PKI-based encryption on each of the packages and generate encrypted packages using the certificate data; and

a high volume transport component operable to receive the encrypted packages and send each package to its intended recipient based on the account data.

51. The system of claim 50, wherein the data files represent at least one of bills and statements.

52. The system of claim 50, wherein each recipient comprises a local agent operable to receive and decrypt the encrypted package.

53. The system of claim 50, wherein the account data includes an email address.

54. The system of claim 50, wherein the high volume transport component comprises an email server.

55. The system of claim 50, wherein the high volume encryption component encrypts the packages using a public key associated with the recipient.

56. A method of sending content using an email client, the content being encrypted in accordance with PKI--based encryption, the method comprising the steps of:

(a) creating the content;

(b) launching a local agent associated with the email client;

(c) passing the content and an address of a recipient to the local agent;

(d) selecting at least one dissemination rule for the content;

(e) obtaining a public key associated with the recipient;

(f) encrypting the content using the public key and a private key;

(g) wrapping the encrypted content with the at least one dissemination rule thereby creating a package;

(h) transmitting the package to a control server which is operable to forward the package to the recipient.

57. The method of claim 56, wherein the content is at least one of an email message, an email attachment, a document, a business transaction, a graphic and streaming audio or video.

58. The method of claim 56, wherein the local agent comprises an application specific interface that provides an interface to the email client.

59. The method of claim 56, wherein the local agent is launched in response to user input.

60. The method of claim 56, wherein the dissemination rule comprises at least one of do not copy, do not print, do not forward and self-destruct.

61. The method of claim 56, further comprising automatically obtaining the public key of the recipient by accessing the control server.

62. The method of claim 61, wherein the control server accesses at least one of a certificate authority server and a LDAP directory service.

63. The method of claim 56, further comprising notifying the recipient of an awaiting package.

64. The method of claim 63, wherein the recipient is notified suing at least one of voice, fax, email and pager.

65. The method of claim 56, wherein the control server stores the package until the package is requested by the recipient.

66. The method of claim 56, wherein the control server causes a unique tracking number to be assigned to the package.

67. The method of claim 56, wherein the local agent communicates automatically with the control server.

68. A method of receiving content using an email client, the content being encrypted in accordance with PKI--based encryption, the method comprising the steps of:

(a) receiving a notification that a package is awaiting downloading, the package comprising encrypted content and at least one dissemination rule;

(b) launching a local agent associated with the email client;

(c) logging on to a control server via the local agent;

(d) downloading the package;

(e) launching a local agent-controlled window; and

(d) decrypting the content within the window in accordance with the dissemination rule.

69. The method of claim 68, wherein the notification is received via at least one of voice, fax, email and pager.

70. The method of claim 68, wherein the content is at least one of an email, an email attachment, a business transaction, a document and a graphics file.

71. The method of claim 68, wherein the local agent communicates with the email client via an application specific interface.

72. The method of claim 68, wherein the local agent is an applet dynamically downloaded via the control server.

73. The method of claim 72, wherein the package is downloaded and stored within the memory allocation of the applet.

74. The method of claim 68, wherein the local agent communicates with the control server to cause the package to be downloaded.

75. The method of claim 68, wherein the encrypted content is stored in the same encrypted form even after being viewed.

76. The method of claim 68, wherein the local agent communicates with the control server before the package is downloaded to authenticate the recipient.

77. A method of automatically implementing PKI-based encryption between a sender and a recipient, the method comprising the steps of:

(a) associating a sender local agent with a sender electronic device, the sender electronic device being capable of connection to the Internet;

(b) associating a recipient local agent with a recipient electronic device, the recipient electronic device being capable of connection to the Internet;

(c) providing a control server, the control server capable of being in communication with both the sender local agent and recipient local agent;

(d) receiving, by the sender local agent, content generated on the sender electronic device;

(e) generating, by the sender local agent, a package of encrypted content using PKI-based encryption by obtaining at least one public key from one of the control server and a local register;

(f) sending the package to the control server;

(g) receiving the package at the control server and notifying the recipient of an awaiting package;

(h) receiving, by the recipient local agent, the package from the control server;

(i) launching a recipient local agent-controlled window;

(j) decrypting the encrypted content in the package; and

(k) displaying the decrypted content within the recipient local agent-controlled window.

78. The method of claim 77, further comprising storing the package in a database accessible to the control server.

79. The method of claim 77, further comprising dynamically downloading at least one of the sender local agent and recipient local agent as an applet from the control server.

80. The method of claim 77, further comprising providing an application specific interface associated with at least one of the sender local agent and the recipient local agent.

81. The method of claim 77, further comprising providing a PKI server operable to at least one of generate public-private key-pairs and access keys via a LDAP service.

82. The method of claim 77, further comprising providing an audit database.

83. The method of claim 77, further comprising assigning a unique tracking number to the package.

84. The method of claim 77, further comprising launching the sender local agent from within an email application.

85. The method of claim 77, further comprising embedding at least one dissemination rule in the package.

86. The method of claim 85, wherein the dissemination rule includes at least one of do not copy, do not print, do not forward and self-destruct.

87. The method of claim 77, wherein the content is at least one of an email, an email attachment, a streaming media file, and an XML file.

88. The method of claim 77, wherein at least one of the sender local agent and recipient local agent is operating system independent.

89. The method of claim 77, further comprising controlling at least one of security, authentication, tracking, confirmation and archiving of the package.

90. A digital audio file, comprising:

a pre-audio identification portion;

an unencrypted audio message;

an encrypted content portion; and

a tag portion.

91. The digital audio file of claim 90, wherein the audio is formatted in accordance with the MP3 standard.

92. The digital audio file of claim 90, wherein the unencrypted audio message includes a notification to a listener regarding use of the digital audio file.

93. The digital audio file of claim 92, wherein the unencrypted audio message provides a listener with instruction regarding how to obtain listening rights to the audio file.

93. The digital audio file of claim 90, wherein the encrypted content portion comprises audio frames and at least one of digital rights management (DRM) data and public keys.

94. The digital audio file of claim 93, wherein the DRM data comprises at least one of a trial key, a play key, and a song key.

95. A secured content delivery system, comprising:

a control server, the control server operable to receive encrypted content from an electronic network, the encrypted content having been encrypted using an encryption scheme

wherein data necessary to implement the encryption scheme having previously been obtained from the control server;

a database server in communication with the control server, the database server being operable to store the encrypted content and store information indicative of a sender of the encrypted content and an intended recipient of the encrypted content; and

a notification server in communication with at least one of the control server and database server, the notification server being operable to notify the intended recipient that the sender has sent encrypted content,

wherein the data necessary to implement the encryption scheme is obtained without an express command from the sender.

96. A method of automatically implementing encryption between a sender and a recipient, the method comprising the steps of:

(a) associating a sender local agent with a sender electronic device, the sender electronic device being capable of connection to the Internet;

(b) associating a recipient local agent with a recipient electronic device, the recipient electronic device being capable of connection to the Internet;

(c) providing a control server, the control server being in communication with both the sender local agent and recipient local agent, but not necessarily at the same time;

(d) receiving, by the sender local agent, content generated on the sender electronic device;

(e) generating, by the sender local agent, a package of encrypted content using an encryption scheme by obtaining data necessary to implement the encryption scheme from one of the control server and a local register;

(f) sending the package to the control server;

(g) receiving the package at the control server and notifying the recipient of an awaiting package;

(h) receiving, by the recipient local agent, the package from the control server;

(i) launching a recipient local agent-controlled window;

(j) decrypting the encrypted content in the package; and

(k) displaying the decrypted content within the recipient local agent-controlled window.

97. The method of claim 96, further comprising storing the package in a database accessible to the control server.

98. The method of claim 96, further comprising dynamically downloading at least one of the sender local agent and recipient local agent as an applet from the control server.

99. The method of claim 96, further comprising providing an application specific interface associated with at least one of the sender local agent and the recipient local agent.

100. The method of claim 96, wherein the encryption scheme is PKI-based encryption and wherein the method further comprises providing a PKI server operable to at least one of generate public-private key-pairs and access keys via a LDAP service.

101. The method of claim 96, further comprising providing an audit database.

102. The method of claim 96, further comprising assigning a unique tracking number to the package.

103. The method of claim 96, further comprising launching the sender local agent from within an email application.

104. The method of claim 96, further comprising embedding at least one dissemination rule in the package.

105. The method of claim 104, wherein the dissemination rule includes at least one of do not copy, do not print, do not forward and self-destruct.

106. The method of claim 96, wherein the content is at least one of an email, an email attachment, a streaming media file, and an XML file.

107. The method of claim 96, wherein at least one of the sender local agent and recipient local agent is operating system independent.

108. The method of claim 96, further comprising controlling at least one of security, authentication, tracking, confirmation and archiving of the package.